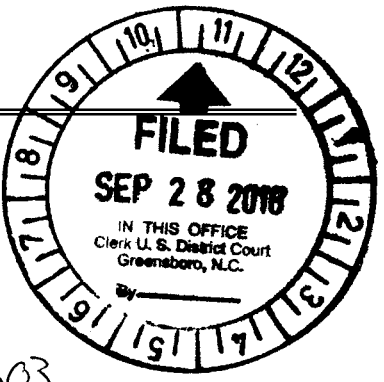

UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

CERTAIN ELECTRONIC DEVICES LOCATED AT 727 MCDOWELL RD, ASHEBORO, N.C.

Case No. 1:18MJ303

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Certain Electronic Devices, more fully described in Attachment A, attached hereto and made part hereof

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

evidence and fruits of violations of 18 U.S.C. § 1029(a)(1), (3), and (4), and § 1343, all of which are more particularly described in Attachment B, attached hereto and made a part hereof.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1029(a)(1),(3),(4)	(1) Production, Use, or Trafficking in Counterfeit Access Devices, (3) With Intent to Defraud 15 or more Counterfeit and Unauthorized Access Devices, (4) Possession of Device Making Equipment, and (1343) Wire Fraud
18 U.S.C. § 1343	

The application is based on these facts:
See the attached affidavit, attached hereto and made a part hereof

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Stephen Greer, USSS Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/28/2018

Judge's signature

City and state: Winston-Salem, North Carolina

The Hon. Joi Elizabeth Peake, United States Magistrate
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF CERTAIN ELECTRONIC DEVICES LOCATED AT 727 MCDOWELL RD, ASHEBORO, N.C.	Case No. 1:18MJ303

AFFIDAVIT

I, Stephen Greer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of certain electronic devices currently in the possession of the Randolph County Sheriff's Office, 727 McDowell Road, Asheboro, N.C. Those devices are a laptop computer portable storage device—specifically,

a. One black and gray Toshiba laptop computer, serial number 5C071660W

b. One black and silver HP Pavilion All in One desktop computer, serial number 8CC5450FLG, and

c. One rose gold iPhone 8 Plus, SEID number 040A42DBB2448001727204317594376657 34CE0F429BCC46.

These devices are further described in Attachment A, and will collectively be referred to herein as the SUBJECT DEVICES. The SUBJECT DEVICES are currently in law enforcement possession in Asheboro, N.C., and the extraction sought from that property of electronically stored information is described in Attachment B.

2. I have been a Special Agent with the United States Secret Service (USSS) for over 11 years. I graduated from Auburn University, Auburn, Alabama, in 1999, with a Bachelor's of Arts degree in Criminal Justice. I also enlisted in the United States Army Reserve in 1996, completing Officer Candidate School in 2003, and finally leaving the Army Reserve in 2007, achieving the rank of First Lieutenant in Military Intelligence. I was also a sworn Police officer for the Metropolitan Police Department (MPD) for 3 years prior and the Wake County Sheriff's Office (WCSO) for 3 years prior to my time with the MPD. I base this affidavit on my personal investigation and the investigation of other law enforcement agents involved in this case with whom I have spoken.

3. I have experience in the investigation of thefts, frauds, counterfeiting, and other violations of law. I am currently a member of the

United States Secret Service Fraud Section, which focuses primarily on financial crimes.

4. I have been involved in the execution of a number of search warrants. Materials searched for and recovered during the execution of these search warrants include but are not limited to the following: evidence consistent with the manufacturing of fraudulent credit/ATM debit cards, computers and or computer systems, central processing units, wireless communications devices (i.e. cell phones), external and internal storage equipment (i.e. floppy disks, CDs, thumb drives, etc.) or media, terminals or video display units, network devices and peripheral equipment such as magnetic stripe reader/writers, encoders, cables, keyboards, printers, modems or acoustic couplers, automatic dialers, computer-related documentation, and computer data, all of which have been or potentially could have been utilized in the commission of the offense referenced below.

5. I have extensive experience in debriefing defendants, conspirators, witnesses, and informants who have been involved or are involved in illegal fraud related activities.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, officers, and witnesses. This affidavit is intended to show merely that there is

sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts set forth in this affidavit, there is probable cause to believe that the SUBJECT DEVICES described in Attachment A contain evidence and fruits of violations of 18 U.S.C. §§ 1029(a)(1) (production, use, or trafficking in counterfeit access devices), 1029(a)(3) (possess with intent to defraud 15 or more counterfeit and unauthorized access devices), 1029(a)(4) (possession of device-making equipment), and 1343 (fraud by wire), hereinafter described as the SUBJECT OFFENSES. There is also probable cause to believe that the SUBJECT DEVICES described in Attachment A used or intended to be used in committing the SUBJECT OFFENSES, and that the SUBJECT DEVICES contain items illegally possessed, to wit: the means of identification of other persons and illegally possessed banking information.

8. The SUBJECT DEVICES are currently located at the Randolph County Sheriff's Office, 727 McDowell Road, Asheboro, N.C.

PROBABLE CAUSE

9. On August 13, 2018, LifeStore Bank Vice President Brianna Ashley called Boone Police Department Lt. Danny Houck and said her bank had been victimized by a male and female team committing fraud using the

ATM. LifeStore Bank is located in Boone, N.C., and its deposits are federally insured through the FDIC. Ashley told Lt. Houck that she had identified $49,920 in attempted ATM withdrawals and an additional $21,760 in withdrawals that were not caught by their system. Ashley said LifeStore Bank had ATM photos and video identifying the same male and female team repeatedly seen in a tan BMW X-5 automobile.

10. Ashley told Lt. Houck that on August 20, 2018, she was at her residence watching the live stream video of the ATM surveillance via computer. Ashley saw the suspects in the tan BMW X-5 attempt to obtain money from the ATM and immediately contacted Lt. Houck, who then directed Boone Police to locate, stop, and arrest the suspects. Lt. Houck said the suspects were stopped, identified as FELTON MCLOYD NORRIS and YENEYDER DEL SOCORRO NORRIS, and arrested approximately an hour later, charged with state offenses of Credit Card/Automatic Teller Machine Fraud. Lt. Houck also stated that the vehicle and driver, FELTON MCLOYD NORRIS, matched the still photos Ashley had presented him from prior ATM fraud incidents at LifeStore Bank.

11. Det. Katrina Eller, Boone Police Department, told me she interviewed FELTON MCLOYD NORRIS, who agreed to speak to the detective and immediately accused his wife, YENEYDER DEL SOCORRO

NORRIS, of all wrongdoing. FELTON MCLOYD NORRIS claimed to be acting on her behalf, simply receiving the cards and PIN numbers from her, then operating the ATM at her instruction. FELTON MCLOYD NORRIS told Det. Eller that he was not sure of where the cards were coming from, but stated that his wife would receive boxes via UPS with a return label from Colombia.

12. Based on the nature of the crimes, Det. Eller and Lt. Houck seized the NORRIS'S BMW X-5 automobile. They also searched that vehicle in an attempt to inventory its contents as required by law. The following is a partial list of the items discovered in their vehicle:

a. Eleven credit cards in the map pocket behind the driver's seat;

b. Ten credit cards in glove box;

c. ATM receipts from Highland Bank;

d. $500 in $20 bills in the passenger door;

e. A purse containing $2,200 in $20 bills;

f. $100 in a clutch inside the purse;

g. Three cell phones;

h. One blue piece of paper with 4-digit numbers found in a cup;

i. Two Western Union receipts, each in the amount of $1,000, in driver's door pocket;

j. One ATM receipt from Forcht Bank in Lexington, Kentucky; and

k. One ATM receipt from University of Kentucky Federal Credit Union, Lexington, Kentucky.

13. Det. Eller told me that based on what they found in the vehicle, she and Lt. Houck believed a search of the NORRIS'S residence would provide even more evidence of crimes similar in nature to those committed in Boone, N.C., based on their training and experience. The officers further stated that, based on their training and experience, suspects such as the NORRISES seldom keep all of their fraudulent documents on their persons, so that in the event the documents or cards are confiscated by authorities, they can continue to perpetrate the fraud at a different location.

14. Det. Eller told me she contacted the Randolph County Sheriff's Office and spoke with Detective Steven Nunn. According to Det. Eller, Det. Nunn was able to assist with the swearing out the affidavit for the search warrant and subsequently executing the search warrant.

15. Lt. Houck said that early on August 21, 2018, Det. Nunn obtained and executed the search warrant on 1927 Fuller Mill Road North, Thomasville, N.C. Below is a partial list of what was discovered at the residence:

a. Four Bancolombia maestro credit cards;

b. One misprinted American Express Business Card Bancolombia;

c. One blank credit card with a chip;

d. One Toshiba Computer, serial number 5C071660W;

e. One HP All in One computer, serial number 8CC5450FLG;

f. One iPhone 8 plus (code 991027) , SEID NUMBER 040A42DBB2448001727204317594376657 34CE0F429BCC46;

g. Deftun brand magnetic stripe reader/encoder;

h. One credit card embosser;

i. One access device card printer;

j. Twenty-seven blank access device cards;

k. Forty-two 3M brand card overlays;

l. Three partial boxes of blank access device cards

m. Four packs of rollers for embossing machine;

n. One Fargo brand access device card printer; and

o. Four card overlays.

16. Based on my training and experience, items such as the SUBJECT DEVICES listed in Attachment A (which includes items in Paragraph 15 d-f above) are commonly used by those trafficking in counterfeit credit or debit cards in multiple ways. For example, magnetic stripe reader/encoders, such as the Deftun model found at the residence, are connected to a laptop computer, so that stolen credit or debit account numbers and other identity information are re-encoded on the magnetic stripe of stolen or counterfeit access devices.

17. Storage devices and those found in computers are commonly used to store names, account numbers, and other authentication features associated with the possession, use, and trafficking of counterfeit credit or debit cards.

18. Wireless telephones are commonly used by those possessing, using, and trafficking in counterfeit credit or debit cards. Suspects send or

receive the stolen account credit or debit account numbers using email or text. The telephones are also used to take pictures and record locations of compromised banks and show a history of where suspects were successful in obtaining money through fraudulent means.

TECHNICAL TERMS

19. Based on my training and experience the below listed terms mean the following as used in this Affidavit:

a. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* Title 18 U.S.C. § 1030(e)(1).

b. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral

input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

e. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a

user's computer a particular IP address that is used each time the computer accesses the Internet.

h. The terms "records," "documents," and "materials" include all information recorded in any form and by any means, including writings, drawings, photographs, audio-recordings, and digital data.

j. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may

also include global positioning system ("GPS") technology for determining the location of the device.

k. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

l. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the SUBJECT DEVICES listed in Attachment A have the following capabilities:

a. The Toshiba Laptop computer has the capability to store records and information, access the Internet, and store and execute computer software.

b. The rose gold iPhone 8 Plus is functions as a Wireless Telephone, as described above, which can be used to access the Internet and can be assigned IP Addresses by Internet Service Providers.

c. The HP All in One computer has the capability to store records and information, access the Internet, and store and execute computer software.

21. In my training and experience, examining data stored on devices of this type can reveal, among other things, evidence of who possessed or used such devices, and evidence of data related to the commission of the SUBJECT OFFENSES.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose

many parts of the SUBJECT DEVICES to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion on to a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICES described

in Attachment A to seek evidence of the SUBJECT OFFENSES, as described in Attachment B.

Respectfully submitted,

Stephen Greer
Special Agent
United States Secret Service

Subscribed and sworn to before me on: 9/28/2018

The Hon. Joi Elizabeth Peake
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched consists of the SUBJECT DEVICES, further described as:

a. One black and gray Toshiba laptop computer, serial number 5C071660W

b. One black and silver HP Pavilion All in One desktop computer, serial number 8CC5450FLG, and

c. One rose gold iPhone 8 Plus, SEID number 040A42DBB2448001727204317594376657 34CE0F429BCC46.

The SUBJECT DEVICES are currently in the custody of the Randolph County Sheriff's Office, 727 McDowell Road, Asheboro, N.C. This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the SUBJECT DEVICES described in Attachment A that relate to violations of 18 U.S.C. §§ 1029(a)(1) (production, use, or trafficking in counterfeit access devices), 1029(a)(3) (possess with intent to defraud 15 or more counterfeit and unauthorized access devices), 1029(a)(4) (possession of device-making equipment), and 1343 (fraud by wire), involving FELTON MCLOYD NORRIS and YENEYDER DEL SOCORRO NORRIS, as follows:

a. lists of identity information;

b. any information concerning counterfeit credit or debit cards/access devices;

c. any information related to sources of counterfeit credit or debit cards/access devices (including names, addresses, phone numbers, or any other identifying information);

d. any information related to the purchase or sale of counterfeit credit or debit cards/access devices;

e. any information related to the manufacture of counterfeit credit or debit cards/access devices, and software programs used to aid

in the manufacture of counterfeit credit or debit cards/access devices;

f. any information regarding any printing device that has been attached to the SUBJECT DEVICES or otherwise connected to the SUBJECT DEVICES wirelessly;

g. information relating to the use of counterfeit and unauthorized credit or debit cards;

h. any information recording FELTON MCLOYD NORRIS and YENEYDER DEL SOCORRO NORRIS's schedule or travel;

i. any photographs and videos relating to counterfeit and unauthorized credit or debit cards or access devices;

j. all information reflecting content of communications sent or received by FELTON MCLOYD NORRIS and YENEYDER DEL SOCORRO NORRIS relating to counterfeit credit or debit cards/access devices, including electronic mail, instant messages, and electronic chats and teleconferencing.

k. Information relating to the possession, use, or transfer of any means of identification of any other person without lawful authority.

2. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.